"Wired World: Cyber Security and the US Economy"
Hearing before the Joint Economic Committee
June 21, 2001

Opening Statement
Senator Robert F. Bennett
Senate Ranking Republican Member

Good morning, and thank you for joining us today as we take a closer look at the issue of cyber security within our increasingly "wired world." During this hearing, we will explore current and future cyber threats to U.S. economic and national security. We also will examine whether the current policies governing cyber security and critical infrastructure protection are sufficient.

The National Intelligence Council will begin by placing the cyber threat over the next fifteen years in the context of globalization. Next, we have a distinguished panel of four representatives from the private sector who will discuss the following: (1) the unintended security issues related to interconnectivity; (2) industry initiatives to mitigate cyber security risks; (3) the need for the for the United States to focus on cyber security in a strategic way; and (4) how strong public–private partnerships can protect our information infrastructures.

Over the past ten years, the world has undergone dramatic technological changes. As technology systems rapidly evolve, most notably the Internet, so has the risk. The benefits of technology are easy to understand. Improved communication means a growth of commerce, expanded free trade and a more closely integrated world.

However, this increased reliance on information technology creates a complicated set of threats to U.S. national and economic security. The enormous proliferation of connectivity and technology now means that potential adversaries no longer need traditional military tools to attack or disrupt the U.S. economy. The tangled web of networks is a potential launching pad for attacks, espionage and viruses by almost anyone around the world. Computer viruses, like the "Love Bug" can cause global damage and disruption. Some of these computer networks and information systems operate parts of critical infrastructures once only accessible by the military. For example, in early May, hackers appearing to originate in China routed themselves through servers in Oklahoma and California and found their way into the California power grid. While the hackers did not cause any blackouts, the potential damage could have been significant.

The world wired together by the Internet is based on computer network connections and powerful communications nodes that are literally redefining the geography of commerce and communication. When we think of national security, we think of making our borders secure. However, on the Internet, borders disappear. In addition, eighty-five percent of U.S. critical infrastructures, such as telecommunications, energy, banking, and transportation systems, are owned by the private sector. In an interconnected world, the private sector is on the front line.

It is important to remember that the Internet was built for sharing, <u>not</u> security. It is inherently open and decentralized. This openness can be costly, though. Computer Economics, a California-based research firm, reports that computer viruses in 2000 cost American businesses over $17 billion. Unfortunately, no one really knows what was lost in terms of intellectual property through espionage, hacking, or foreign intelligence services.

If we leave this hearing with one idea it should be this: The physical world that Rand McNally and other mapmakers introduced us to must not dominate our strategic thinking for the next century. Instead, we - Congress, the executive branch and the private sector - must view

the emerging geography from a strategic perspective. Attempts to map the Internet reveal a world where physical geography disappears. We must resist the temptation to think about the Internet in a traditional context of geographic boundaries.

Over the past several years, there have been many efforts to understand the security associated with cyber-based threats. All too often, however, the complex issues of cyber security and infrastructure protection are overshadowed by the attention paid to hacking exploits and website defacements. It is time that we finally turn to the more strategic security challenges to our economic and national security. We need to take a fresh look at U.S. cyber security infrastructure protection policy. Thank you.

-30-